

# Diseño de un Plan de Contingencia para el Sistema de Gestión de Turnos Desarrollado por la Empresa CIEL Ingeniería S.A.S.

Diego Andrés Quiroz Ramírez

Universidad Piloto de Colombia, Bogotá-Colombia

diegoq182@hotmail.com

**Abstract-** This document presents the design of a contingency plan for a Sistema de Gestión de Turnos, which is a client-server application developed by CIEL Ingeniería S.A.S. for them clients. Three main phases are covered: the activation and notification phase to activate the plan and determine the extent of damages; the recovery phase to restore system operations; and the reconstruction phase to ensure that the system is validated through testing and that normal operations are resumed.

**Palabras claves-** aplicación, cliente, continuidad de negocio, disponibilidad, plan de contingencia, sistema de turnos, seguridad informática, servidor.

## I. INTRODUCCIÓN

En la actualidad los sistemas de información y las tecnologías de la información representan un alto valor agregado para muchas organizaciones a nivel mundial, por lo tanto resulta importante garantizar su confidencialidad, integridad y disponibilidad; garantizando la continuidad de las operaciones después de ocurrido un suceso que afecte el ciclo normal del servicio. Debido a esto, se hace necesario crear planes de continuidad de negocio, es decir, un conjunto de procedimientos y estrategias definidos para asegurar la reanudación oportuna y ordenada de los procesos del negocio, generando un impacto mínimo o nulo ante una contingencia. El estándar internacional para la continuidad del negocio, ISO 22301, la define como la “capacidad (de una organización) de continuar la prestación de productos o servicios en los niveles predefinidos aceptables tras incidentes de interrupción de la actividad”.

El National Institute of Standards and Technology (NIST) desarrolla y emite estándares, pautas y otras publicaciones para ayudar a las agencias federales a implementar la Federal Information Security Management Act (FISMA) de 2002 y a administrar programas efectivos para la protección de los sistemas de información. La publicación especial NIST 800-34 proporciona instrucciones, recomendaciones y consideraciones para la planificación de contingencia de sistema de información federal. La planificación de contingencia se refiere a medidas provisionales para recuperar los servicios del sistema de información después de una interrupción. Las medidas provisionales pueden incluir la reubicación de los sistemas de información y las operaciones en un sitio alternativo, la recuperación de las funciones del sistema de información utilizando

equipos alternativos o el desempeño de las funciones del sistema de información utilizando métodos manuales. Este documento aborda recomendaciones de planificación de contingencia para un sistema cliente-servidor específico desarrollado por la empresa CIEL Ingeniería S.A.S. perteneciente al sector privado, ubicada en la ciudad de Bogotá-Colombia; la cual brinda soluciones tecnológicas de atención inteligente a sus clientes en todo el país. Uno de sus principales portafolios de servicios incluye el Sistema de gestión de Turnos, el cual han desarrollado para mejorar la experiencia de atención al usuario.

Como en todo sistema de información, es importante garantizar la seguridad de sus activos. Este artículo define el proceso de ejecución de un plan de contingencia que los clientes de CIEL Ingeniería pueden aplicar para desarrollar y mantener un programa de planificación de contingencia viable para el Sistema de Gestión de Turnos. Se brindan estrategias de recuperación completas para asegurar que el sistema pueda restaurarse de manera rápida y efectiva luego de una interrupción. Se debe asegurar el mantenimiento del plan, es decir, un documento que se actualice regularmente para mantenerse actualizado con las mejoras del sistema y los cambios en la organización del cliente.

## II. CATEGORIZACIÓN DE SEGURIDAD DEL SISTEMA DE GESTIÓN DE TURNOS

Basados en la Federal Information Processing Standards (FIPS) 199 – Standards for Security Categorization of Federal Information and Information Systems, que define tres niveles de impacto potencial en organizaciones o individuos en caso de que haya una violación de la seguridad (es decir, una pérdida de confidencialidad, integridad o disponibilidad), el Sistema de Gestión de Turnos se clasifica como un sistema de impacto potencial moderado, es decir, se podría esperar que la pérdida de confidencialidad, integridad o disponibilidad tenga un efecto adverso serio en las operaciones de la organización, los activos de la organización o individuos.

Un efecto adverso serio significa que, por ejemplo, la pérdida de confidencialidad, integridad o disponibilidad podría: (i) causar una degradación significativa en la capacidad de la misión en la medida y en la duración en que la organización pueda realizar sus funciones principales, pero la efectividad de las funciones se reduce significativamente; (ii) ocasionar daños significativos a los activos de

la organización; (iii) dar lugar a una pérdida financiera significativa; o (iv) causar un daño significativo a las personas que no implique la pérdida de vidas o lesiones graves que pongan en peligro la vida.

Sin embargo, esta clasificación puede variar dependiendo de la organización en la cual se implementa el sistema de Gestión de Turnos, ya que puede ser considerado de bajo impacto para algunos clientes y no afecte significativamente la confidencialidad, integridad o disponibilidad de su modelo principal de negocio.

Los procedimientos en este ISCP son para un sistema de impacto moderado y está diseñado para la recuperación del Sistema de Gestión de Turnos dentro de 24 horas. Este plan no trata el reemplazo o la compra de equipos nuevos, las interrupciones a corto plazo que duran menos de 24 horas; o pérdida de datos en las instalaciones en el sitio o de los niveles de servicio del usuario final.

### III. PLAN DE CONTINGENCIA DEL SISTEMA DE INFORMACIÓN (ISCP)

Es necesario que los servicios provistos por CIEL Ingeniería S.A.S. a sus clientes puedan operar efectivamente sin interrupciones excesivas. Este Plan de Contingencia del Sistema de Información (ISCP) establece procedimientos integrales para recuperar el Sistema de Gestión de Turnos de manera rápida y efectiva después de una interrupción del servicio, debido a que este sistema de información puede ser fundamental en el desarrollo de los procesos de misión y negocios de sus clientes.

La información contenida en este ISCP proporciona una representación precisa de la aplicación, su hardware, software y componentes de telecomunicaciones. Además este documento identifica la criticidad del sistema en lo que se relaciona con la misión de los clientes, y que las estrategias de recuperación identificadas proporcionarán la capacidad de recuperar la funcionalidad del sistema en el método más conveniente y rentable para mantener su nivel de disponibilidad. Se recomienda probarlo al menos una vez al año. Este documento se modificará a medida que se produzcan cambios y permanecerá bajo el control de versiones, de acuerdo con la política de planificación de contingencia de cada cliente.

Este ISCP para el Sistema de Gestión de Turnos establece procedimientos para recuperar Sistema de Gestión de Turnos luego de una interrupción. Se establecen los siguientes objetivos del plan de recuperación:

- Maximizar la efectividad de las operaciones de contingencia a través de un plan establecido que consta de tres fases:

La fase de activación y notificación: describe el proceso de activación del plan basado en los impactos de interrupción y la notificación al personal de recuperación.

La fase de recuperación: detalla el proceso de implementación sugerido para que los equipos de recuperación restauren las operaciones del sistema en un sitio alternativo destinado por el cliente o si es posible en la ubicación principal.

La fase final, reconstrucción: incluye actividades para probar y validar la capacidad y funcionalidad del sistema. También describe las acciones que se pueden tomar para devolver el sistema a su estado normal de funcionamiento y prepararlo contra futuras interrupciones.

- Identificar las actividades, recursos y procedimientos para llevar a cabo la restauración del Sistema de Gestión de Turnos después de una interrupción prolongada de las operaciones normales.
- Asignar responsabilidades al personal designado por el cliente y brindar orientación para la recuperación del Sistema de Gestión de Turnos luego de períodos prolongados de interrupción en las operaciones normales.

### IV. SUPOSICIONES

Las siguientes suposiciones son utilizadas para desarrollar este ISCP:

- El Sistema de Gestión de Turnos se ha establecido como un sistema de impacto moderado, de acuerdo con FIPS 199.
- Las copias de seguridad actuales del software y los datos del sistema están intactas y disponibles en las instalaciones de almacenamiento fuera de las instalaciones del cliente en CIEL Ingeniería S.A.S.
- El Sistema de Gestión de Turnos no funciona y no se puede recuperar dentro de 24 horas.
- El administrador del Sistema de Gestión de Turnos ha sido identificado y capacitado en sus funciones de respuesta de emergencia y recuperación; disponibles para activar el Plan de Contingencia para el Sistema de Gestión de Turnos.

El Plan de contingencia para el Sistema de Gestión de Turnos no se aplica a las siguientes situaciones:

- Recuperación general y continuidad de la misión comercial del cliente. El Plan de Continuidad del Negocio (BCP) y el Plan de Continuidad de las Operaciones (COOP) abordan la continuidad de las operaciones de negocio.
- Emergencias de evacuación del personal. El Plan de Emergencia del Ocupante (OEP) direcciones empleado evacuación.

### V. CONCEPTOS DE OPERACIÓN

A continuación se proporcionan detalles sobre el Sistema de Gestión de Turnos, una descripción general de las tres fases del ISCP (Activación y Notificación, Recuperación y Reconstrucción), y una descripción de los roles y responsabilidades del personal del cliente durante una activación de contingencia.

#### A. Descripción del sistema

El sistema de Gestión de Turnos, desarrollado por CIEL Ingeniería S.A.S., es una solución tecnológica de tipo cliente-servidor centralizado que cuenta con elementos de hardware y software. Está compuesto por un sitio web instalado en el servidor de aplicaciones dado por el cliente, tres bases de datos y posee autenticación de usuarios ante un directorio activo.

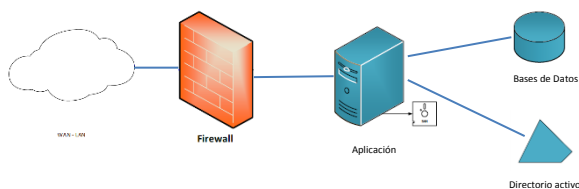


Fig. 1. Diagrama del Sistema.

Algunas de los requisitos y políticas de seguridad que deben garantizar los clientes para la instalación del sistema son:

- Equipo servidor, Intel Xeon CPU E5-2667 v2 @ 3.30Ghz, 100GB DD, 16GB RAM.
- Sistema operativo Windows Server 2012 Standard IIS 8.5 (Compatibilidad AppPool 32 Bits) Cliente Oracle 32 Bits (4.121.1.0).
- Se debe contar con usuario y password de acceso a los servidores, para realizar conexión remota y realizar los procedimientos de despliegue de las aplicaciones.
- Para la conexión a los servidores de base de datos, se debe tener un usuario y password de conexión a los diferentes esquemas utilizados.
- Se deben asignar permisos de acceso a los segmentos de red donde se encuentran los servidores.
- El cliente debe garantizar equipos con especificaciones mínimas para la instalación del sistema

Posee un software complementario que se instala en dos equipos designados en cada lugar donde se realiza atención a sus usuarios finales: un equipo utilizado para la generación e impresión de los turnos y otro equipo utilizado para el llamado de turnos en pantalla.

El acceso a la aplicación se realiza mediante cualquier navegador web a través de la red interna de cada cliente, cada usuario se valida contra directorio activo para el ingreso desde un equipo de escritorio o portátil.

Los servicios de mantenimiento de software se deben realizar mediante el acompañamiento directo de CIEL ingeniería S.A.S. para garantizar la configuración adecuada del sistema, el cual entrega la documentación técnica del sistema para servir de referencia a sus clientes.

Se recomienda realizar un backup periódico de los esquemas de base de datos, la periodicidad es directamente definida por las políticas internas de cada cliente. Así mismo, realizar backup de los servidores virtuales de aplicación configurados en HyperView con periodicidad recomendada de (1) mes.

### B. Definición de las tres fases

Este ISCP se ha desarrollado para recuperar y reconstituir el Sistema de Gestión de Turnos utilizando un enfoque de tres fases. Este enfoque garantiza que los esfuerzos de recuperación y reconstrucción del sistema se realicen en una secuencia metódica para maximizar la efectividad de los esfuerzos de recuperación y reconstrucción y minimizar el tiempo de interrupción del sistema debido a errores y omisiones. Las tres fases de recuperación del sistema son:

**Fase de activación y notificación:** la activación del ISCP se produce después de una interrupción que puede extenderse razonablemente más allá del RTO establecido para un sistema. El evento de interrupción puede provocar daños severos en las instalaciones que albergan el sistema, daños graves o pérdida de equipos, u otros daños que generalmente resultan en pérdidas a largo plazo.

Una vez que se activa el ISCP, se notifica a los propietarios y usuarios del sistema sobre una posible interrupción a largo plazo, y se realiza una evaluación exhaustiva de la interrupción del sistema. La información de la evaluación de interrupción se presenta a los clientes del sistema y se puede utilizar para modificar los procedimientos de recuperación específicos.

**Fase de recuperación:** la fase de recuperación detalla las actividades y los procedimientos para la recuperación del sistema afectado. Las actividades y los procedimientos se escriben a un nivel en el que un técnico calificado puede recuperar el sistema sin un conocimiento especializado del sistema. Esta fase incluye procedimientos de notificación y escalamiento para comunicar el estado de recuperación a los propietarios y usuarios del sistema.

**Fase de reconstrucción:** la fase de reconstrucción define las acciones tomadas para probar y, validar la capacidad y la funcionalidad del sistema en la ubicación original nueva o permanente. Esta fase consta de dos actividades principales: validación exitosa de la reconstrucción y desactivación del plan.

Durante la validación, el sistema se prueba y valida como operativo antes de que la operación vuelva a su estado normal. Los procedimientos de validación pueden incluir pruebas de funcionalidad o regresión, pruebas de concurrencia y/o validación de datos. El sistema se declara recuperado y operativo por los propietarios del sistema al completar con éxito las pruebas de validación.

La desactivación incluye actividades para notificar a los usuarios el estado operativo del sistema. Esta fase también trata la documentación durante del esfuerzo de recuperación, la finalización del registro de actividades, la incorporación de las lecciones aprendidas en las actualizaciones del plan y la preparación de recursos para cualquier evento futuro.

### C. Roles y responsabilidades

El ISCP establece varias funciones para el soporte de recuperación y reconstrucción del Sistema de Gestión de Turnos. Las personas o equipos asignados a los roles del ISCP son entrenados para responder a un evento de contingencia que afecte al Sistema de Gestión de Turnos.

**El director del ISCP** será el responsable general de la administración del plan, esta persona será definida por cada cliente, generalmente asignado al gerente de tecnología de la información o administrador de los sistemas de información.

**El coordinador del ISCP** será el responsable de supervisar el progreso de recuperación y reconstrucción, iniciar cualquier notificación o comunicación necesaria con CIEL Ingeniería S.A.S, y establecer la coordinación con otros equipos de recuperación y reconstrucción apropiados. Esta persona será establecida por el cliente, generalmente dicha responsabilidad es asignada al administrador técnico del Sistema de Gestión de Turnos.

**El punto de recuperación técnica** será definido por cada cliente desde la última copia de respaldo que se tenga hasta el momento. CIEL Ingeniería realizará acompañamiento en la fase de recuperación y reconstrucción del sistema.

## VI. ACTIVACIÓN Y NOTIFICACIÓN

La fase de activación y notificación define las acciones iniciales tomadas una vez que se detectó una interrupción del Sistema de Gestión de Turnos o parece ser inminente. Esta fase incluye actividades para notificar al personal de recuperación, realizar una evaluación de interrupciones y activar el ISCP. Al finalizar la fase de

activación y notificación, el personal del ISCP para el Sistema de Gestión de Turnos estará preparado para realizar las medidas de recuperación.

#### *A. Criterios de activación y procedimiento*

El ISCP del Sistema de Gestión de Turnos puede activarse si se cumple uno o más de los siguientes criterios:

- El tipo de interrupción indica que del Sistema de Gestión de Turnos estará inactivo durante más de 48 horas.
- El lugar donde actualmente se encuentra instalado el Sistema de Gestión de Turnos ha sufrido un daño severo y es posible que no esté disponible dentro de 48 horas.
- Otros criterios dados por el cliente que afecte la disponibilidad del servicio a causa de la interrupción del sistema.

Las siguientes personas o roles pueden activar el ISCP si se cumple uno o más de estos criterios:

El gerente de tecnología de la información del cliente o en su defecto la persona que cumpla la función de administrador técnico del sistema.

#### *B. Notificación*

El primer paso en la activación del ISCP para el Sistema de Gestión de Turnos es la notificación al personal de soporte encargado del funcionamiento del sistema. La información de contacto para los puntos de contacto de operaciones POC apropiados se incluye en el listado de números de contacto de servicio al cliente de CIEL Ingeniería S.A.S.

Para el Sistema de Gestión de Turnos, se utiliza el siguiente método y procedimiento para las notificaciones:

Inicialmente se realiza notificación por parte del personal de soporte técnico, encargado del monitoreo, seguimiento y administración funcional, al coordinador del ISCP del sistema de gestión de turnos. El coordinador del ISCP posteriormente notifica a la mesa de servicios de CIEL Ingeniería S.A.S. que se encarga de registrar el incidente para proceder a programar el acompañamiento por parte de especialistas en el sistema para la implementación de la etapa de recuperación

#### *C. Evaluación de la interrupción*

Después de la notificación, es necesaria una evaluación exhaustiva de la interrupción del servicio para determinar el alcance de la interrupción, cualquier daño y el tiempo de recuperación esperado. Esta evaluación de interrupción se lleva a cabo por CIEL Ingeniería S.A.S una vez que el cliente proporcione toda la información, logs y datos necesarios para realizar un análisis completo de las posibles causas de la interrupción del servicio, identificación de la posibilidad de una interrupción adicional o daño, determinar los elementos que deberán reemplazarse y el tiempo estimado para restablecer el servicio a las operaciones normales. Los resultados de la evaluación se proporcionan al Coordinador de ISCP para ayudar en la coordinación de la recuperación del sistema de Gestión de Turnos.

## **VII. RECUPERACIÓN**

La fase de recuperación proporciona operaciones de recuperación formales que comienzan después de que se haya activado el ISCP, se

hayan completado las evaluaciones de interrupciones, se haya notificado al personal y se hayan movilizado los equipos apropiados y el personal de CIEL Ingeniería S.A.S a las instalaciones del cliente. Las actividades de la fase de recuperación se enfocan en implementar estrategias de recuperación para restaurar las funcionalidades del sistema, reparar daños y reanudar las capacidades operativas en la ubicación original o en una ubicación alternativa. Al finalizar la fase de recuperación, el Sistema de gestión de Turnos será funcional y capaz de realizar las funciones identificadas en la sección V.

#### *A. Secuencia de Actividades de Recuperación*

Las siguientes actividades se desarrollan durante la recuperación del sistema de Gestión de Turnos:

- 1) Identificar la ubicación de recuperación (instalaciones del cliente)
- 2) Identificar los recursos necesarios para realizar procedimientos de recuperación;
- 3) Recuperar la copia de seguridad y la instalación de las bases de datos necesarias para el funcionamiento del sistema.
- 4) Recuperar hardware y sistema operativo (si es necesario)
- 5) Recuperar de copia de seguridad y la instalación de la aplicación principal necesaria para el funcionamiento del sistema.

#### *B. Procedimientos de recuperación*

Los siguientes procedimientos se proporcionan para la recuperación del Sistema de gestión de Turnos en la ubicación original o alterna dada por el cliente. Los procedimientos de recuperación se describen por equipo y se deben ejecutar en la secuencia presentada para mantener un esfuerzo de recuperación eficiente.

CIEL Ingeniería S.A.S. proporciona los procedimientos generales para la recuperación del sistema desde las copias de seguridad. La instalación del sistema estará a cargo de los especialistas designados por CIEL Ingeniería S.A.S. en acompañamiento del coordinador del ISCP del cliente y los especialistas técnicos a cargo del soporte del sistema. El cliente garantizará que los equipos utilizados para la recuperación del sistema cumplan con los requisitos mínimos para su instalación.

El procedimiento se resume en cuatro partes principales:

- Restauración de las bases de datos necesarias para el funcionamiento del sistema desde la última copia de seguridad creada por el cliente.
- Instalación de los sitios web en el servidor de aplicación.
- Comunicación entre bases de datos y el servidor de aplicación, la cual debe garantizar el cliente.
- Actualización de los grupos de usuarios en directorio activo.

#### *C. Notificación del proceso de recuperación*

Durante la etapa de recuperación, cada procedimiento es documentado y suministrado por CIEL Ingeniería al coordinador del ISCP para que éste sea el encargado de coordinar y supervisar la implementación final en el ambiente de producción de su organización, de acuerdo las políticas de seguridad y procedimientos internos.

## VIII. RECONSTRUCCIÓN

La reconstrucción es el proceso mediante el cual se completan las actividades de recuperación y se reanudan las operaciones normales del sistema. Si la instalación original no se puede recuperar, las actividades en esta fase también pueden aplicarse a la preparación de una nueva ubicación permanente para soportar los requisitos de procesamiento del Sistema de Gestión de Turnos. Se debe determinar si el sistema ha sufrido un cambio significativo y requerirá una reevaluación y una nueva implementación. La fase consta de dos actividades principales: validación exitosa de la reconstrucción y desactivación del plan.

### A. Pruebas de Funcionalidad y Validación de Datos

Es el proceso empleado para garantizar que los archivos o las bases de datos se hayan recuperado completamente en la ubicación permanente. Adicionalmente se garantiza que el sistema se encuentre funcionando correctamente.

Los siguientes procedimientos se utilizan para determinar la funcionalidad del sistema, así mismo que los datos están completos y actualizados hasta la última copia de seguridad disponible:

- Correcto ingreso a la aplicación mediante el navegador web y validación de usuarios.
- Correcto ingreso al software complementario para la generación e impresión de turnos.
- Generación, llamado y atención de turnos de pruebas en las oficinas de atención.
- Verificación en la información en los reportes históricos del Sistema de Gestión de Turnos.

Se debe identificar si las pruebas son exitosas o no, y registrar los resultados obtenidos

### B. Declaración de Recuperación

Al completar con éxito la prueba y validación, el cliente declarará formalmente que los esfuerzos de recuperación están completos, y que el Sistema de Gestión de Turnos se encuentra en normal operación. El Coordinador de ISCP notificará a los POC comerciales y técnicos sobre la declaración del Sistema de Gestión de Turnos.

### C. Notificaciones a los usuarios

Al regresar a las operaciones normales del sistema, se notificará a los usuarios del Sistema de Gestión de Turnos mediante los procesos de comunicación interna establecidos por el cliente (por ejemplo: correo electrónico, mensaje de difusión, llamadas telefónicas, etc.).

### D. Almacenamiento externo de datos

Es importante que todas las copias de seguridad de las bases de datos, sitio web y medios de instalación utilizados durante la recuperación se retomen a la ubicación de almacenamiento de datos fuera de la ubicación principal.

Los procedimientos para devolver las copias de respaldo a su ubicación de almacenamiento de datos fuera de la ubicación principal son propios de cada cliente, el cual debe garantizar que se sigan cumpliendo las recomendaciones de copias de seguridad periódicas dadas anteriormente. CIEL Ingeniería S.A.S. siempre dispone de todos los medios de instalación del sistema, los cuales implementará en los casos que sean necesarios.

### E. Datos de Respaldo

Tan pronto como sea razonable después de la recuperación, se debe hacer una copia de seguridad completa del sistema y almacenar una nueva copia del sistema operativo actual para futuros esfuerzos de recuperación. Esta copia de seguridad completa se mantiene con otras copias de seguridad del sistema, la cual se recomienda que se almacenen fuera de la ubicación principal del cliente.

Los procedimientos para realizar una copia de seguridad completa del sistema son:

- Copia de respaldo de las bases de datos del Sistema de Gestión de Turnos.
- Copia de respaldo de la carpeta donde está contenido el sitio web instalado en el servidor de aplicación.

### F. Documentación de eventos

Es importante que todos los eventos de recuperación estén bien documentados, incluidas las acciones tomadas y los problemas encontrados durante el esfuerzo de recuperación y reconstrucción, y las lecciones aprendidas para la inclusión y actualización de este ISCP. Es responsabilidad de cada equipo o persona de ISCP documentar sus acciones durante los esfuerzos de recuperación y reconstrucción y proporcionar dicha documentación al Coordinador de ISCP, el cual recopilará la siguiente información:

- Los registros de actividad (incluidos los pasos de recuperación realizados y por quién, la hora en que se realizaron los pasos, y cualquier problema o inquietud encontrada al ejecutar las actividades);
- Resultados de las pruebas de funcionalidad
- Lecciones aprendidas durante el proceso y hallazgos encontrados.
- Reporte post-implementación.

### G. Desactivación

Una vez que se hayan completado todas las actividades y se haya actualizado la documentación, la autoridad designada por el cliente desactivará formalmente el esfuerzo de recuperación y reconstrucción del ISCP. La notificación de esta declaración se proporcionará a todas las áreas comerciales y técnicas.

## IX. CONCLUSIONES

- Resulta importante para la empresa CIEL Ingeniería tener disponible un plan de contingencia para el Sistema de Gestión de Turnos, el cual pueda suministrar a sus clientes como guía de preparación ante una eventual situación que afecte la disponibilidad de sus servicios.
- Los planes de contingencia para sistemas de información permiten salvaguardar, en casos de interrupción del servicio, los sistemas importantes para cualquier organización, entre ellos: sistemas cliente/servidor; sistemas de telecomunicaciones o sistemas de mainframe.
- El Sistema de Gestión de Turnos se ha clasificado como un sistema de impacto potencial moderado debido a que en algunos casos la interrupción prolongada del sistema puede afectar significativamente la confidencialidad, integridad o disponibilidad de la información relacionada con el modelo principal o misión de negocio de los clientes.

## X. REFERENCIAS

- [1] NIST 800-34 Rev. 1, Contingency Planning Guide For Federal Information Systems, 2010.
- [2] FIPS PUB 199, Standards for Security Categorization of Federal Information and Information Systems, 2004.
- [3] ISO 22301:2012 Seguridad de la Sociedad - Requisitos para el Sistema de Administración de Continuidad de Negocios.
- [4] Federal Information Security Management Act (FISMA), 2002, Public Law 107-347.



**Diego A. Quiroz Ramirez.** Ingeniero Electrónico graduado de la Universidad Industrial de Santander. Cuenta con 4 años experiencia en el sector de las TICs. Conocimientos relacionados con soporte e implementación de aplicaciones, bases de datos, servidores, sistemas operativos Windows y Linux. Conocimientos en IPv6 certificado por LACNIC. Capacitado para analizar, utilizar, adaptar y gestionar, los diferentes aspectos de las

telecomunicaciones, de acuerdo con los requerimientos contemporáneos de las empresas y organizaciones, en un ambiente global de competencia y de convergencia, a nivel empresarial, regulatoria, de redes y de servicios. Profesional solidario, responsable, ético, creativo, tolerante, comprometido con el trabajo, cuidadoso con el medio ambiente, vinculado a redes temáticas y con capacidad para trabajar en equipos interdisciplinarios.